ABSTRACT OF THE DISCLOSURE

[00125]   A computing platform (10) protects system firmware (30) using a manufacturer certificate (36). The manufacturer certificate binds the system firmware (30) to the particular computing platform (10). The manufacturer

5   certificate also stores configuration parameters and device identification numbers. A secure run-time platform data checker (200) and a secure run-time checker (202) check the system firmware during operation of the computing platform (10) to ensure that the system firmware (30) or information in the manufacturer certificate (36) has not been altered. Application software files (32)

10 and data files (34) are bound to the particular computing device (10) by a platform certificate (38). Configuration parameters may be stored in a data file (34) with an associated platform certificate (38).